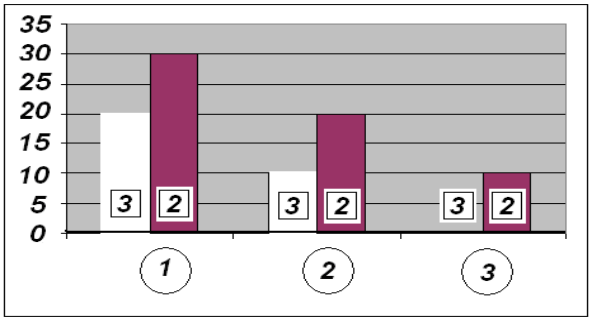

Рисунок 8 — Рівні гармонік, виміряних в точках 1, 2 і 3, згідно з рис. 3 при А= мінус 10 дБ, В= мінус 30 дБ

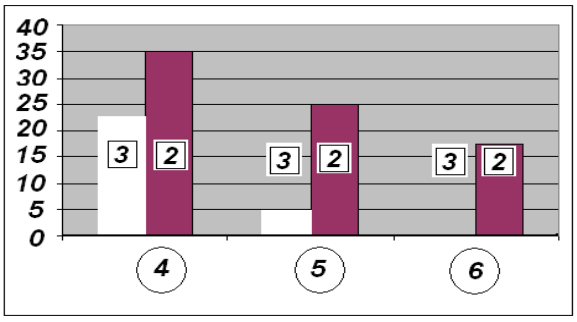

Рисунок 9 — Рівні гармонік, виміряних в точках 4, 5 і 6, згідно з рис. 3 при А= мінус 10 дБ, В= мінус 20 дБ

Згідно з результатами дослідження чітка ідентифікація ЗП як електронного об'єкта (рівень другої гармоніки значно перевищує рівень третьої), незважаючи на послаблення зондуючого сигналу і суттєве зменшення чутливості приймачів щодо другої і третьої гармонік, відбулася лише у випадку дослідження плоскої спіральної антени, навантаженої на напівпровідниковий елемент. Значний вплив оточуючих напівпровідникових і МОМ- структур підтверджує хибна ідентифікація напівпровідникового елемента (діода КД 522А без технологічних виводів) як завадового об'єкта, оскільки рівень 3-ї гармоніки суттєво перевищував рівень 2-ї (див рис. 6, 7).

IV Висновок

Плоска двозаходова спіральна антена, навантажена на напівпровідниковий елемент, завдяки широкосмуговості дає можливість чіткої ідентифікації електронного об'єкта, при цьому шкідливий вплив оточуючих напівпровідникових і МОМ структур мінімізується, оскільки імітатор ЗП випромінює достатньо великі рівні гармонік порівняно з гармоніками оточуючих нелінійних елементів.

Література: ***1.*** *Дорошко В. А., Чекатков А. А. Методы и средства защиты информации. К.: "Юниор", 2003. – 504 с.* ***2.*** *Марков Г. Т., Сазанов Д. М. Антенны. М.: «Энергия », 1975. – 366 с.* ***3.*** *Юрцев О. А., Рунов А. В., Казарин А. Н. Спиральные антенны. М.: «Сов. радио», 1974. – 224 с.*

УДК 681.3.06; 681.5; 621.391

ОСОБЛИВОСТІ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ ЗА ТЕХНОЛОГІЄЮ IP/MPLS

Володимир Кононович, Сергій Гладиш*, Микола Тардаскін**
*Академія зв'язку України, *Одеська національна академія зв'язку ім. О. С. Попова, **Одеський регіональний центр ТЗІ ВАТ "Укртелеком"*

Анотація: **Визначено порядок проведення робіт та технічні вимоги до комплексної системи захисту державних інформаційних ресурсів в телекомунікаційній мережі загального користування, побудованих за технологією IP/MPLS. Розглянуто особливості реалізації комплексної системи захисту інформації.**
Summary: **It is defined the works order and technical requirements for the complex information security system of state information resources in the public telecommunication network based on IP/MPLS technology. The specific terms of realization of the complex information security system are considered.**
Ключові слова: **Захист інформації, державний інформаційний ресурс, телекомунікаційна система, технологія IP/MPLS.**

I Вступ

Захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах приділяється все більша увага при зростанні ролі інформації в усіх сторонах життя особи, суспільства, виробництва й держави та поширенню загроз і ризиків інформаційної, економічної, екологічної, технологічної тощо, безпеки в рамках національної безпеки України.

Дана робота присвячується вирішенню проблем побудови й функціонування комплексної системи захисту державних інформаційних ресурсів та інформації, яка циркулює в телекомунікаційних системах загального користування, захисту телекомунікаційних послуг та інформації населення, організацій та підприємств, яка передається мережами.

Статтею 31 Конституції України, Законом України «Про телекомунікації» [1] та іншими законами гарантується «Охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж». Винятки можуть бути встановлені лише судом у випадках, передбачених законом.

У минулому столітті, за часу панування декадно-крокових й координатних телефонних станцій, аналогових систем зв'язку та слабо автоматизованих систем керування електрозв'язком ці права були забезпечені технічними й організаційно-правовими заходами. Проблема захисту інформації не стояла так гостро, як зараз. Головними загрозами інформаційній безпеці були несанкціонований фізичний доступ до ліній та систем зв'язку й витік інформації каналами побічних електромагнітних витоків та наведення (ПЕМВН). Фізичний захист систем та мереж зв'язку, організаційно-технічні засоби захисту забезпечувались підприємствами зв'язку, а для контролю ПЕМВН було досить роботи відповідних підрозділів спеціальних державних органів. Захищений документальний електрозв'язок успішно здійснювався телеграфними системами та мережами. Телеграми мали певну юридичну силу, якщо були завірені начальниками поштових чи телеграфних відділень. Створені тоді системи захисту інформації не були явно виділеними, вони були органічно вбудовані в систему технічної експлуатації електрозв'язку і становили її невід'ємну частину. Ефективність цієї системи була наглядно продемонстрована під час останніх виборів до парламенту, коли для оперативної передачі даних з виборчих дільниць до центральної виборчої комісії довіреною виявилась лише мережа телеграфного зв'язку.

Наразі пропускна здатність телеграфних мереж вже давно не задовольняє потреб суспільства і держави, а сучасні телекомунікаційні системи відрізняються не лише термінологією, колосальною пропускною здатністю та широкою номенклатурою інформаційно-телекомунікаційних послуг, а й суттєво ширшим переліком загроз та підвищеними вимогами до їх інформаційної безпеки. Змінилось і призначення телекомунікацій. Із сфери обслуговування населення вони перетворились у потужний фактор виробництва й перспективну сферу бізнесу.

Розширення пропускної здатності цифрових мереж в Україні випереджало розвиток систем їх інформаційної безпеки, особливо на перших етапах цифровізації. Перші цифрові телефонні станції (EWSD, 5ESS тощо), цифрові магістралі були побудовані без засобів захисту інформаційних ресурсів, а управління ними обмежувалось національним сегментом. На другому етапі, при розвитку телекомунікацій за технологіями ATM, Frame relay, системи технічного захисту були впроваджені фрагментарно на цифрових вузлах комутації та системах управління телекомунікаціями. На нинішньому етапі розпочато впровадження мереж наступного покоління (Next Generic Network – NGN) і, в першу чергу, мереж за технологією IP/MPLS. Надалі, при будь-якому впровадженні нових технологій першочергова увага до безпеки стала обов'язковою. При впровадженні нових технологій більш адекватно оцінюються загрози їхній інформаційній безпеці і створюються системи інформаційної безпеки з потрібним раціональним рівнем захищеності інформаційних ресурсів й гарантій захисту. В результаті досягається зниження ризиків інформаційної безпеки до прийнятного рівня як у телекомунікаційних системах, так і в інформаційно-телекомунікаційних системах, до яких останні входять.

Для виконання положення статті 17 Конституції України про забезпечення її економічної та інформаційної безпеки Законом «Про телекомунікації» додатково встановлюється низка вимог (стаття 9):

- зняття інформації з телекомунікаційних мереж заборонене, крім випадків, передбачених законом;
- оператори, провайдери телекомунікацій зобов'язані вживати відповідно до законодавства технічні та організаційні заходи із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами.

Захищаючи права людини, Конституція України статтею 32 не допускає "збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини». Тому в телекомунікаціях, статтею 34 Закону «Про телекомунікації» щодо захисту інформації про споживача стверджується: «Оператори, провайдери телекомунікацій повинні забезпечувати й нести відповідальність за схоронність відомостей щодо споживача, отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо; вживати заходів для недопущення несанкціонованого доступу до телекомунікаційних мереж та інформації, що передається цими мережами».

Передбачена відповідальність за невиконання вказаних статей Закону. Стаття 41 передбачає, що персонал оператора, провайдера телекомунікацій, тобто всі працівники, які перебувають з ним у трудових відносинах, несуть «відповідальність за порушення вимог законодавства України щодо збереження таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, а також інформації з обмеженим доступом щодо організації та функціонування телекомунікаційних мереж в інтересах національної безпеки, оборони та охорони правопорядку". В даній статті ми не торкаємося питань захисту інформації з обмеженим доступом, що належить державі, але розглядаються засоби захисту державних інформаційних ресурсів органів державного управління та самоврядування, які передаються телекомунікаційними мережами.

Метою статті є аналіз особливостей засобів захисту й комплексної системи захисту державних інформаційних ресурсів та інформації користувачів, яка підлягає захисту відповідно до законодавства в телекомунікаційних мережах, побудованих за технологіями IP/MPLS.

ІІ Аналіз порядку виконання робіт з ТЗІ в телекомунікаційній мережі

Сучасні телекомунікаційні мережі розглядаються як надскладна ієрархічна система. До такої системи важко точно застосувати всі етапи існуючого порядку виконання робіт з технічного захисту інформації (ТЗІ) та процедури створення КСЗІ, які розраховані на захист об'єкта інформаційної діяльності за типом «кругової оборони». Телекомунікаційну мережу складає велика кількість об'єктів типу вузлів комутації, з'єднаних між собою каналами або сегментами магістралі, які також треба вважати об'єктами, де обробляється, тимчасово зберігається та передається інформація. До існуючого порядку розробки доцільно додати етапи й процедури, які б враховували ієрархічний та розподілений характер телекомунікаційної мережі, а також інтеграцію інформаційних та телекомунікаційних мереж. Формально можна розбити порядок виконання робіт на три загальних цикли, кожен з яких розділявся б на етапи відповідно до вимог ДСТУ 3396.0-96 [2], а етапи виконувались би стадіями, в порядку, що передбачається ДСТУ 3396.1-96 [3]. Цикли виконання робіт можуть бути такими:

1) загальний цикл створення технічного завдання (ТЗ) та плану захисту (ПЗ) телекомунікаційної мережі в цілому як складової інформаційно-телекомунікаційної системи. У цьому циклі проводиться обстеження телекомунікаційної мережі та інформаційної системи, в інтересах якої функціонує телекомунікаційна мережа, аналізуються загрози інформаційним ресурсам, визначаються вимоги до системи захисту інформації саме в телекомунікаційній мережі, обирається мережний функціональний профіль захисту, розробляються засоби реалізації комплексної системи захисту державних інформаційних ресурсів (КСЗІР) в телекомунікаційній мережі;

2) загальний цикл декомпозиції телекомунікаційної мережі на взаємопов'язані об'єкти інформаційної діяльності (ОІД), раціональної інтерпретації загальних вимог до захищеності інформації за вимогами до системи захисту інформації в ОІД, розробка оптимального розподілу засобів захисту за ОІД;

3) загальний цикл виконання робіт з ТЗІ на кожному з телекомунікаційних ОІД відповідно до вимог ДСТУ 3396.0-96 та ДСТУ 3396.1-96.

Недоліком такого розподілу робіт є те, що не враховується ієрархічний характер телекомунікаційних мереж та нерівномірний розподіл механізмів захисту за рівнями ієрархії. Це стосується, перш за все, штатних засобів захисту, що вбудовуються в кожні пристрої, системи, технології, які в сукупності утворюють телекомунікаційну мережу. Модель взаємодії відкритих систем передбачала сім рівнів ієрархії: фізичний, канальний, мережний, транспортний, сеансовий, представницький та прикладний. Розвиток мікроелектроніки, мініатюризація пристроїв, програмна й мікропрограмна реалізація функцій та, навпаки, апаратна реалізація типових програмно виконуваних функцій привели до інкапсуляції деяких рівнів. На сьогодні в телекомунікаційних мережах виділяють чотири-п'ять ієрархічних рівнів, які тепер називають площинами: абонентського доступу (інкапсулює фізичний та канальний рівні), комутації (мережний рівень), програмного управління (рівень транспорту), управління мережею та створення й надавання послуг (інкапсулює сеансовий, представницький та прикладний рівні).

Тому в другому та третьому загальних циклах виконання робіт з ТЗІ мають додаватись наступні етапи:

- аналіз та ініціалізація штатних засобів захисту, вбудованих в елементи телекомунікаційної мережі на її ієрархічних рівнях;
- реалізація організаційних, організаційно-технічних та програмно-технічних заходів, які доповнюють штатні засоби захисту до повної КСЗІР згідно з обраним мережним функціональним профілем захисту;
- розробка порядку й засобів взаємодії механізмів захисту на кожному з ієрархічних рівнів із засобами управління та контролю функціонування КСЗІР;
- прив'язка ієрархії засобів захисту інформації до конкретних фізично-географічних ОІД.

Діючі нормативно-правові документи сфери захисту інформації рекомендують аналізувати рівень

захищеності інформації, виявляти нові загрози й ризики інформаційної безпеки, розробляти ТЗ на вдосконалення й модернізацію КСЗІР, повторюючи весь цикл виконання робіт [4]. На цьому етапі має значення розвиток штатних засобів захисту, що має призводити до ефективнішого розподілу задач захисту між штатними та додатковими механізмами захисту.

Проілюструємо запропонований порядок робіт на прикладі КСЗІР телекомунікаційної мережі, побудованій за технологією IP/MPLS.

III Характеристика умов функціонування телекомунікаційної мережі

Технологія багатопротокольної комутації міток – MPLS (Multiprotocol Label Switching) була створена наприкінці 90-х років, реалізується поверх системи з IP (Internet Protocol) на транспортному рівні і прийшла на заміну технології ATM (Asynchronous Transfer Mode) [5]. Технологія MPLS представляє собою набір протоколів, включаючи протоколи сигналізації й управління, які дозволяють створювати й управляти сучасними високошвидкісними мережами. MPLS здійснює комутацію трафіка за допомогою наперед розставлених міток, що прискорює цей процес і надає ряд додаткових можливостей, таких як контроль трафіка та організація віртуальних приватних мереж (VPN). Як і до всіх сучасних телекомунікаційних технологій до неї висуваються вимоги передачі різних видів інформації (аудіо, відео, мови й даних) загальними каналами зв'язку за допомогою уніфікованого транспортного механізму та забезпечення при цьому заданої якості обслуговування – QoS (Quality of Service). При цьому, технологія IP/MPLS надає додаткові сервісні можливості [6]:

- введення різних категорій потоків класів обслуговування CoS;
- можливість забезпечення заданої якості обслуговування QoS для різних категорій;
- надання єдиного транспортного механізму для передачі різних видів інформації та можливість роботи з різними мережними технологіями і протоколами (Frame Relay, IP, ATM, Ethernet).

Важливими задачами, які доводиться вирішувати в процесі побудови мереж IP/MPLS, є задачі аналізу й вибору засобів захисту інформації та інформаційних ресурсів, а також взаємоузгодження штатних засобів захисту інформації на транспортному та мережному рівнях телекомунікаційних систем з додатковими засобами захисту, які створюються поза транспортним рівнем телекомунікаційної системи в рамках КСЗІР у телекомунікаційних мережах і яка реалізується на рівні управління телекомунікаційними мережами й наданням послуг.

Мережі на базі технології IP/MPLS будуть складатись з таких мережних елементів, як маршрутизатори, комутатори, DWDM – системи Add-Drop мультиплексори, фотонні або оптичні комутатори. Багатопротокольна комутація міток (MPLS) [7 – 9] реалізується набором процедур, які доповнюють пакети мережного рівня «стеком міток» для перетворення їх у помічені пакети, та мікро програмним забезпеченням маршрутизаторів, які підтримують протокол MPLS. Такий маршрутизатор називається LSR (Label Switching Router). Для передачі поміченого пакету певним каналом LSR підтримує методику кодування й аналізу помічених пакетів. IP/MPLS не залежить від мережних протоколів, але використовує і протокольно залежні процедури для IPv4 й IPv6. Фізично LSR можуть бути на ATM - комутаторах та інших комутаторах.

Стек міток є послідовністю рівневих записів, кожен з яких має довжину 4 байти. Варіант формату запису та місце стека міток в пакеті показані на рис. 1.

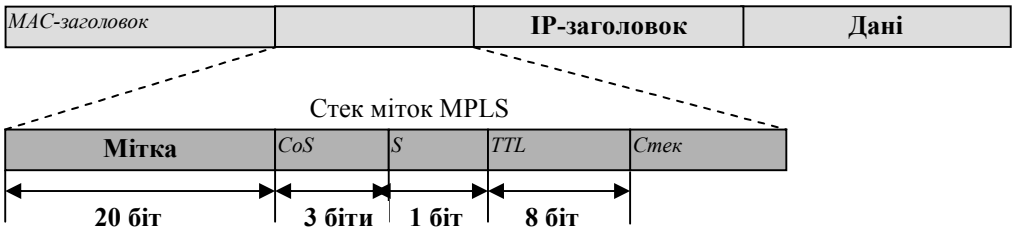

Рисунок 1 – Формат запису стека міток

Кожен запис стека міток містить у собі такі поля: час життя пакета (TTL – 8 біт); кінцівка стека (поле S – 1 біт). Цей біт встановлюється рівним 1 для останнього запису у стеку міток, і нулю для всіх інших записів; сервіс (CoS – 3 біти). Сервіс буде використовуватись для визначення якості інформації, що передається, а також для вказівки пріоритетності користувачів: Значення поля мітки (20 біт) містить код мітки. Приклади коду міток: значення «0» вказує, що пере адресація пакета має бути проведена згідно з IPv4-заголовком; значення «2» вказує, що пере адресація пакета має бути проведена згідно з IPv6-

заголовком; значення «1» вказує, що пакет має бути доставлений локальному модулю для обробки, який переадресує пакет згідно з міткою в його стеці. Мітка присвоюється комутатором, який знаходиться на нижчому (мережному) рівні.

Коли отримано помічений пакет, аналізується значення мітки на верхівці стека, в результаті якого визначається наступний крок, куди буде переадресовано пакет і операція, яка має бути виконана із стеком до переадресації. Це може бути заміна мітки на верхівці стека, видалення запису із стека, заміщення верхньої позиції у стеці і занесення туди однієї чи більше нових записів. Додатково до визначення наступного кроку можна отримати дані про інкапсуляцію вихідної інформації та інші дані.

Коли остання мітка видаляється зі стека, то подальша обробка пакета здійснюється на основі його заголовка мережного рівня. Це може бути, наприклад, IP - заголовок. Тип мережного протоколу визначається за інформацією з останнього запису стека міток.

Аналіз штатних засобів захисту, вбудованих в елементи телекомунікаційної мереж, побудованої за технологією IP/MPLS, зводиться до наступних результатів щодо інформаційних ресурсів та інформації.

Проміжні вузли мають бути здатні посилати протокольно залежні повідомлення про помилки чи критичні ситуації (що виявляються обладнанням) для помічених пакетів. Якщо проміжний LSR визначає, що помічений пакет не може бути доставлено (приміром, коли час закінчився чи місце призначення не доступне), то він має сформувати повідомлення про помилку чи критичну ситуацію у вигляді пакету мережного рівня (так званого ICMP-повідомлення) для передачі його відправнику поміченого пакету. Єдиним засобом, який має проміжний LSR для ідентифікації мережного рівня, є аналіз верхніх записів стеку та заголовка мережного рівня. Для формування й передачі ICMP-повідомлення конкретний LSR визначає, що конкретний помічений пакет є IP - пакетом і прокладає маршрут до місця відправника цього пакета. Якщо пакет не може бути переадресований з будь-якої причини, або його протокол мережного рівня не може бути ідентифіковано, або не існує правил для обробки випадків виявлення помилок, то тоді пакет має бути без коментарів відкинуто.

Одним з ключових критеріїв, які відображають якість роботи мережі, є її сталість та відмовостійкість. Механізми захисту з'єднань від можливих аварій забезпечуються на мережному рівні перемиканням навантаження на резервний канал за час менший за 50 мс (резервування 1 + 1). На транспортному рівні з єдиним рівнем управління ці механізми інтегруються за допомогою сигналізації. На транспортному рівні варіант резервування 1 + 1 реалізується віртуально і дозволяє суттєво зменшити час відновлення мережі від пошкоджень. Це забезпечується таким чином. Між кожними кінцевими комутаторами LSR при створенні з'єднання LSR автоматично створюється додаткове з'єднання LSR, яке встановлюється іншим маршрутом. В критичній ситуації для перевстановлення втраченого з'єднання LSR необхідно лише перемкнути основний LSR на резервний, який вже створено й чекає в гарячому резерві.

Уніфікована багатопротокольна комутація міток – GMPLS (Generalized MPLS) – надає можливість уніфікувати управляючу частину цієї технології [7]. Технологія GMPLS є універсальною сигнальною технологією для пакетних і волоконно-оптичних мереж. Вона дозволяє створити єдину універсальну транспортну магістраль, яка здатна обслуговувати будь-який трафік користувачів на різних швидкостях та протоколах доступу. Зокрема, в ній можливі варіанти організації захисту від пошкоджень мережі типу M + N, при якому M альтернативних з'єднань LSR захищаються N альтернативними з'єднаннями. При цьому кількість альтернативних N з'єднань може бути більшою, рівною чи меншою ніж M. Альтернативні з'єднання можуть встановлюватись без резервування ресурсів мережі, а при переключенні на нього трафіка забираються у менш пріоритетних з'єднань. При виникненні аварійної ситуації не потрібно додаткового часу на розповсюдження сигнальних повідомлень. Час витрачається лише на розповсюдження аварійного повідомлення від точки виявлення аварії до точки переключення маршрутизації на початковому комутаторі LSR.

Що стосується інформаційної безпеки в мережі на базі технології IP/MPLS, то аналіз документів, таких як [8 – 13] виділяє наступні особливості. В технології IP/MPLS не передбачається будь-якої додаткової безпеки, крім тієї, яка закладена в архітектурі MPLS або в структурі протоколу мережного рівня.

Деякі з маршрутизаторів можуть здійснювати процедури безпеки, які залежать від заголовка мережного рівня, що займає фіксоване місце відносно заголовка канального рівня. Інкапсуляція нижніх рівнів у верхніх виключає проведення обміну між MPLS та процедурами й протоколами канального рівня. Це може перешкоджати виконанню деяких процедур безпеки. На практиці може бути необхідною взаємодія між механізмами безпеки канального та транспортного рівня. Не тільки адміністративно, але й технологічно домени первинної мережі зв'язку та транспортної мережі можуть не співпадати. Але, приміром, при виявленні й владнанні інцидентів з інформаційною чи фізичною безпекою може бути необхідною взаємодія між КСЗІР цих мереж. У свою чергу інкапсуляція мережного рівня технологією MPLS перешкоджає обміну між рівнем управління телекомунікаціями й надаванням послуг та мережним рівнем.

Аналогічно, в цьому випадку необхідно організовувати взаємодію між системами захисту поза рівнем управління.

В технології IP/MPLS закладені певні, але не повні елементи послуг безпеки типу «невідмовності від авторства» та «невідмовності від приймання». Мітка MPLS заноситься у стек «автором мітки», а читає й інтерпретує її LSR, який є «читачем мітки». Але стек міток не має ніяких засобів для визначення того, хто є дійсним автором конкретної мітки. Якщо помічені пакети прийняті від ненадійних джерел, або прийнято від LSR, від якого така мітка не може поширюватись, то пакети можуть бути маршрутизовані незаконним чином. Вирішення цієї проблеми лежить поза можливостями транспортного рівня мережі і має бути вирішене на рівні управління мережею та надаванням послуг.

Можуть виникати питання захисту інформації, які будуть пов'язані з реалізацією робочих параметрів в системах вимірювання в мережах MPLS [11]. Системи вимірювання, які оцінюють робочі характеристики мереж MPLS відповідно до визначення параметрів, що приведені в Рекомендації [11], повинні обмежувати вимірюваний трафік відповідними рівнями для запобігання зловживань (наприклад, DoS-атака). Оператори повинні заздалегідь погоджувати прийнятний рівень трафіка вимірювань. Системи, що контролюють трафік користувача з метою вимірювання, мають забезпечувати збереження конфіденційності інформації користувача. Системи, які намагаються провести вимірювання, можуть використовувати криптографічне гешування, щоб встановити, чи не введено порушником додатковий трафік.

Функції підсистеми OAM (експлуатації та технічного обслуговування) можуть підсилити безпеку мереж MPLS [12]. Наприклад, функції перевірки зв’язності (CV), які визначаються в рекомендації [12], можуть виявити помилкові з'єднання і не допустити передачу трафіка, призначеного для одних користувачів іншим користувачам.

Захист комутації також може покращити стан безпеки мереж MPLS завдяки функції автоматичної комутації трафіка від ущкоджених (компрометованих) LSP до тих LSP, які функціонують належним чином [13]. Це дозволить запобігти несанкціонованому витоку трафіка.

IV Загрози інформаційним ресурсам та вибір функціонального профілю захисту

Кінцевою метою заходів безпеки КСЗІР, яка впроваджується в мережі IP/MPLS, є забезпечення надання користувачам високоякісних послуг доступу до телекомунікаційних послуг, забезпечення зв’язності між компонентами мережі IP/MPLS, створення централізованих систем управління мережею та послугами за умов безпеки інформаційних ресурсів та інформації, що передається мережею. *Призначення КСЗІР* полягає у забезпеченні технічного захисту інформації, яка є власністю держави та інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, яка циркулює, обробляється, зберігається та передається мережею IP/MPLS. *Інформація*, яка захищається, *характеризується* наступним. Згідно зі статтею 2 Закону [14] об’єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації. Захисту в системі підлягає:

- відкрита інформація, яка є власністю держави і у визначенні Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами;
- конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі *конфіденційна інформація про фізичну особу;*
- телекомунікаційні послуги та передавання інформації, що надаються населенню, організаціям та підприємствам; технічному захисту підлягає конфіденційна інформація, яка обробляється і зберігається на серверах управління та послуг (бази даних, технологічна інформація, програмне забезпечення).

Потенційні загрози несанкціонованого доступу. Перелік загроз неодноразово наводився у численних публікаціях, але він продовжує змінюватись та уточнюватись. Загальний аналіз загроз проводився на базі рекомендацій Міжнародного союзу електрозв’язку, зокрема Рекомендації МСЕ-Т Е.408 [15]. Аналіз охоплює наступні питання інформаційної безпеки телекомунікацій: нелегальне проникнення (імітація з’єднання); підслуховування; несанкціонований доступ (НСД); втрата або спотворення інформації; не признання авторства; підлог (фальсифікація); відмова в обслуговуванні; технічні канали витоку.

Потенційні загрози мають антропогенну (людський фактор) й техногенну природу, вони можуть бути випадковими й навмисними. Найбільші потенційні загрози несуть несанкціоновані дії: блокування інформації в системі; витік інформації; знищення інформації; несанкціоновані дії; порушення цілісності; несанкціонований доступ до баз даних, технологічної інформації, програмному забезпеченню, фізичним носіям інформації; несанкціоноване користування доступом до мережі IP/MPLS; непередбачена зміна

зовнішніх факторів (електроенергії, кондиціювання, стихійних лих і т.п).

Можливі технічні канали витоку та впливу на інформацію на сьогодні менш актуальні, ніж несанкціонований доступ. Апаратура має відповідати нормам електромагнітної сумісності, що зменшує ймовірність витоку інформації каналами електромагнітного випромінювання й наводок. У багатоканальних системах діє ефект взаємного маскування сигналів випромінювання. Несанкціонований з'йом інформації та вплив на неї може здійснюватися: несанкціонованим доступом шляхом підключення до апаратури по лініям зв'язку, маскуванням під зареєстрованого користувача, подоланням заходів захисту, використанням програм та впровадженням комп'ютерних вірусів; каналами спеціального впливу шляхом формування полів та сигналів з метою зруйнування системи захисту або порушення цілісності інформації.

Згідно з п. 16 діючих «Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [16] захист інформації від витоку технічними каналами забезпечується в системі у разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято власником чи розпорядником інформації.

Офіційних функціональних профілів захисту для телекомунікаційних мереж поки не розроблено. рекомендація [4, 15] пропонує функціональні класи на трьох рівнях безпеки: мінімальний функціональний клас (FC 1); базовий функціональний клас (FC 2); удосконалений функціональний клас (FC 3). Можна вважати доцільним застосовування базового функціонального класу FC 2, якщо в мережі обробляється державний інформаційний ресурс і реалізувати мінімальний функціональний клас FC 1 в інших випадках.

Якщо КСЗІР реалізує базовий функціональний клас безпеки (FC 2), то профіль безпеки утворюється наступними послугами безпеки:

- основна увага приділяється цілісності ресурсів, що зберігаються, та цілісності даних, що передаються;
- реалізуються послуги: автентифікації; управління доступом до адміністративного управління; управління доступом до керованого ресурсу; *автентифікація джерела даних;вибіркова цілісність поля даних;цілісність з'єднання;*аварійний сигнал безпеки, перевірка і відновлення;
- факультативно може надаватись послуга конфіденційності з'єднання та вибіркова конфіденційність поля даних.

Якщо КСЗІР реалізує мінімальний функціональний клас безпеки (FC 1), то профіль безпеки відрізняється тим, що: основна увага надається лише цілісності керованих ресурсів, що зберігаються; серед обов'язкових реалізованих послуг відсутні: *автентифікація джерела даних; вибіркова цілісність поля Даних; цілісність з'єднання;* інші послуги ті ж самі, що й у FC 2, а факультативно може надаватись послуга *цілісність з'єднання* та конфіденційність з'єднання.

V Вимоги до комплексної системи захисту інформації у мережі IP/MPLS

Вимоги до функцій (послуг) забезпечення безпеки. Відкрита інформація під час обробки в системі має зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.

Усім користувачам має бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження. Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, не ідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення. Доступ до конфіденційної інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації не ідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора мають блокуватися. В системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки конфіденційної інформації або позбавлення його такого права. Забезпечення захисту в системі таємної інформації, що не становить державну таємницю, здійснюється згідно з вимогами до захисту конфіденційної інформації.

Вимоги до захисту інформації від несанкціонованого блокування визначаються її власником (розпорядником), якщо інше не встановлено законодавством.

У системі здійснюється обов'язкова реєстрація: результатів ідентифікації та автентифікації

користувачів; результатів виконання користувачем операцій з обробки інформації; спроб несанкціонованих дій з інформацією; фактів надання та позбавлення користувачів права доступу до інформації та її обробки; результатів перевірки цілісності засобів захисту інформації. Забезпечується можливість проведення аналізу реєстраційних даних виключно користувачем, якого уповноважено здійснювати управління засобами захисту інформації і контроль за захистом інформації в системі (адміністратор безпеки). Реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки. Реєстрація спроб несанкціонованих дій з інформацією, що становить державну таємницю, а також конфіденційної інформації про фізичну особу, яка законом віднесена до персональних даних, повинна супроводжуватися повідомленням про них адміністратора безпеки.

Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом.

Передача конфіденційної і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

У системі забезпечується захист інформації від комп'ютерних вірусів, здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації. Контролюється також цілісність програмних та технічних засобів захисту інформації. У разі порушення їх цілісності обробка в системі інформації припиняється.

Послуги, які забезпечують підтримку життєдіяльності (при непередбачуваній зміні зовнішніх факторів) вузлів та захист від несанкціонованого користування послугами мають бути реалізовані з високим рівнем стійкості.

Вимоги до рівня гарантій. Має забезпечуватись 1-й рівень гарантій: безпеки персоналу, стандартизації технологічного середовища, забезпечення спостережливості та керованості технологічного середовища, забезпечення конфіденційності і цілісності інформаційних ресурсів та якості документації.

Технічні заходи з ТЗІ при розробці робочого проекту розширення/будівництва вузла мережі IP/MPLS від ПЕМВН передбачаються системними та системно-технічними методами.

Вимоги до системних та системно-технічних методів. Передбачається використання раціональних методів монтажу, технічних засобів з розв'язуючими і фільтруючими елементами для блокування впливу по технічним каналам, резервних засобів електроживлення (акумулятори, дизель-генератори, задіяння кількох вводів, тощо), дублювання критичних систем та модулів, використання систем запобігання несподіваним впливам зовнішніх факторів та стихійних лих.

VI Особливості реалізації комплексної системи захисту інформації у мережі IP/MPLS

Організаційні та організаційно-технічні заходи з захисту інформації. Для забезпечення захисту інформації в системі створюється КСЗІР, яка призначається для захисту інформації від:

- несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;
- спеціального впливу на найбільш критичні компоненти мережі (серверні, програмні комутатори, пункти управління мережею тощо), який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення цілісності та несанкціонованого блокування інформації.

КСЗІР забезпечує вирішення п'яти задач безпеки: конфіденційність (інформації, що зберігається або переноситься); цілісність даних (захист інформації, що зберігається або переноситься); цілісність системи; звітність (кожен об'єкт повинен бути відповідальним за будь-які дії, які він ініціював; до звітності включається автентифікація, фіксація авторства та управління доступом); готовність (усі легітимні об'єкти повинні одержати коректний доступ до мережі).

Порівняно з вимогами до КСЗІР вітчизняної нормативно-правової бази, згідно з міжнародними рекомендаціями необхідно реалізувати послуги: автентифікації користувача та джерела даних; захист від не визнання участі; аудиторський журнал.

Організація та проведення робіт із захисту інформації в мережі здійснюється службою захисту інформації (СЗІ) [17], яка забезпечує визначення вимог до захисту інформації в мережі, проектування, розроблення і модернізацію системи захисту, виконання робіт з її експлуатації, контролю за станом захищеності, а також організації по реагуванню на інциденти та обробці інцидентів безпеки.

Усе обладнання повинно бути розміщено в будівлях в межах контрольованої території, що має пропускний та внутрішній режими, які відповідають режимним вимогам, що визначено чинними в організації нормативними та розпорядчими документами. Контроль за доступом до приміщень, де знаходяться критичні з точки зору безпеки інформації компоненти вузлів та мережі IP/MPLS, має

забезпечуватися на всіх етапах її життєвого циклу. Порядок доступу до приміщень із визначенням категорій користувачів, які мають право це здійснювати, визначається СЗІ і затверджується керівником організації. Для приміщень, в яких розташовані категорійовані компоненти вузлів та мережі IP/MPLS, мають бути вжиті відповідні заходи із захисту інформації від витоку технічними каналами, достатність і ефективність яких засвідчується актами атестації комплексів технічного захисту інформації для кожного такого приміщення.

Захист інформації на всіх етапах створення та експлуатації системи здійснюється відповідно до розробленого службою захисту інформації плану захисту інформації в системі та *Правил* і *Методик* організації по реагуванню на інциденти й обробки інцидентів безпеки. План захисту інформації в системі містить: завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації; визначення моделі загроз для інформації в системі; основні вимоги щодо захисту інформації та правила доступу до неї в системі; перелік документів, згідно з якими здійснюється захист інформації в системі; перелік і строки виконання робіт службою захисту інформації.

Правила й *Методики* організації по реагуванню на інциденти й обробки інцидентів безпеки включають у себе [18]: виявлення та визначення типу інциденту, області його дії та наслідків; локалізації, тобто зупинку явища й обмеження наслідків інциденту безпеки; ліквідація причини та попередження повторення; відновлення нормальної роботи; перевірка виконання. Згідно з статтею 7 Закону України [14] «Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі». Тому мають бути розроблені також *Правила взаємодії та інформування про інциденти* всіх суб'єктів відносин в ході обробки інцидентів безпеки.

Для організації управління доступом до конфіденційної інформації та компонентів вузлів та мережі IP/MPLS необхідно: розробити та впровадити посадові інструкції користувачів та персоналу вузлів та мережі IP/MPLS, а також інструкції, якими регламентується порядок виконання робіт іншими особами з числа тих, що мають доступ до обладнання; розробити та впровадити розпорядчі документи, щодо правил перепусткового режиму на територію, в будівлі та приміщення, де розташовано обладнання вузлів та мережі IP/MPLS; визначити правила адміністрування окремих компонентів мережі IP/MPLS та процесів, використання ресурсів вузлів, а також забезпечити їх розмежування між різними категоріями адміністраторів; визначити правила обліку, зберігання, розмноження, знищення носіїв конфіденційної інформації; розробити та впровадити правила ідентифікації користувачів та осіб інших категорій, що мають доступ до обладнання вузлів.

Апаратно-програмні заходи захисту вузлів IP/MPLS від НСД до інформації. За сукупністю характеристик – конфігурації апаратних засобів, обчислювальної системи та їхнього фізичного розміщення, кількості різноманітних категорій опрацьованої інформації, кількості та категорій користувачів IP/MPLS можна розглядати як автоматизовану систему класу "3". Мережа IP/MPLS за структурою технічних та програмних засобів, що використовуються, є гетерогенною структурою, має різну топологію, що, відповідно, визначає різні підходи до забезпечення режимів циркулювання інформації та способів доступу до неї. Загальні функціональні вимоги, які протистоять переліченим загрозам, описуються таким набором: підтвердження ідентифікаційної інформації; керований доступ та авторизація; захист конфіденційності (для технологічної інформації та персональних даних – обов'язковий, для інформації, що передається – факультативний); захист цілісності даних; звітність; реєстрація дій; аварійне сповіщення; аудит.

КСЗІР повинна гарантувати користувачам стійкість автоматизованої системи до відмов та можливість проведення заміни окремих її компонентів з одночасним збереженням доступності до окремих вузлів IP/MPLS або до мережі IP/MPLS в цілому. Готовність системи залежить від надійності апаратних та програмних засобів та гарантується узгодженим набором всіх перелічених послуг безпеки.

У мережі IP/MPLS під час зберігання, оброблення та передавання інформації має забезпечуватися *реєстрація дій* користувачів способом, що дозволяє однозначно ідентифікувати користувача, адресу робочого місця, з якого здійснено доступ до об'єктів та час, протягом якого здійснювався доступ. Засоби захисту мають забезпечити необхідний рівень цілісності та конфіденційності інформації в журналах реєстрації центрального вузла із можливим виділенням одного чи декількох серверів аудиту. Статистика роботи користувачів повинна бути спостереженою й доступною для адміністратора безпеки та/або співробітників СЗІ. Журнали реєстрації системи повинні мати захист від несанкціонованого доступу, модифікації або руйнування. КСЗІР повинна забезпечити ідентифікацію користувача з визначенням точки його входу до мережі, однозначно автентифікувати його і зареєструвати результат (успішний чи невдалий) цих подій у системному журналі. У випадку виявлення неавторизованого користувача повинна блокуватися можливість його роботи в мережі.

КСЗІР повинна забезпечувати можливість двох режимів роботи користувача - із конфіденційною інформацією та з відкритою інформацією, гарантуючи в першому випадку доступ до відповідних об'єктів і процесів як з обмеженим доступом, так і до загальнодоступних, а в останньому - тільки до відкритої інформації й блокування будь-якого доступу до об'єктів і процесів з обмеженим доступу. В обох режимах повинна забезпечуватися можливість визначення власниками об'єктів конкретних користувачів або їх групи, яким надається право мати доступ до цих об'єктів.

У передбачених випадках мережа має забезпечити можливості гарантування *конфіденційності* даних, що зберігаються та передаються. Конфіденційна інформація може зберігатися, як на окремих виділених для цього (однорівневих) пристроях - серверах, робочих станціях, запам'ятовуючих пристроях та ін., так і на пристроях, що одночасно зберігають інформацію загального призначення (багаторівневих). КСЗІР повинна забезпечити розмежування доступу користувачів різних категорій до інформації незалежно від способу її групування на однорівневих чи багаторівневих пристроях.

Засоби адміністрування автоматизованої системи управління телекомунікаціями повинні забезпечувати контроль за можливостями встановлення, перегляду, модифікації стратегій управління (наприклад, реалізація управління віртуальними мережами), а комплекс засобів захисту (КЗЗ) - гарантувати забезпечення контролю за цілісністю засобів адміністрування мережі.

Копіювання об'єктів, що містять конфіденційну інформацію, із сервера на робочу станцію користувача дозволяється тільки у випадках, коли це передбачено технологічними процесами обробки інформації. КЗЗ повинен гарантувати, що зазначені процеси перед завершенням своєї роботи забезпечують копіювання цих об'єктів на сервер (якщо в цьому є потреба) і знищують їх на робочій станції способом, що унеможливлює відновлення або відтворення. Під час обробки конфіденційної інформації повинна забезпечуватися можливість відміни окремої операції або певної їх послідовності до стану, що визначено користувачем або передбачено технологією реалізації певних процедур функціональним або системним програмним забезпеченням.

Виведення інформації у текстовому вигляді повинно здійснюватися на зареєстровані в установленому порядку паперовому носії на спеціально виділених для цього пристроях друку. КСЗІР повинна забезпечити контроль за процесом виконання роздрукування інформації з фіксацією в системному журналі: імені користувача, об'єкта, робочої станції та часу, коли здійснюється роздрукування. У разі необхідності можлива фіксація додаткової інформації, що характеризує процес роздрукування і дозволяє його однозначно ідентифікувати. Реалізація функцій копіювання інформації в електронному вигляді на знімні носії інформації та створення резервних копій може здійснюватися тільки уповноваженими користувачами або за дозволом адміністратора безпеки. КСЗІР повинна контролювати процеси в мережі шляхом реєстрації в журналі системи: імені користувача, об'єкта копіювання, робочої станції та часу, коли здійснюється процес копіювання або створення резервної копії. Допускається фіксація додаткової інформації, що характеризує ці процеси і дозволяє їх однозначно ідентифікувати.

Повинна бути реалізована можливість виявлення фактів несанкціонованого доступу до об'єктів та (або) процесів, що потенційно можуть призвести до виникнення загроз для інформації, і забезпечена фіксація в журналі системи: імені користувача, об'єкта та (або) процесу, до якого була спроба доступу, місця та часу, коли виникла загроза. Допускається фіксація додаткової інформації, яка дозволяє однозначно ідентифікувати процеси, що створили загрозу. КСЗІР повинна забезпечити блокування роботи робочих станцій, з яких була здійснена загроза інформації. КСЗІР повинна генерувати аварійне сповіщення безпеки при виникненні критичних інцидентів з безпеки.

Мережа повинна бути у стані, який гарантує *цілісність системи*, а також *даних,* які зберігаються та передаються. Система має гарантувати, що будь-який об'єкт не може відмовитись від відповідальності за будь-які виконані ним дії, а також за їх наслідки.

Висновки

Складність телекомунікаційної мережі як сукупності об'єктів інформаційної діяльності не дозволяє точно витримувати діючий порядок виконання робіт з технічного захисту інформації. Тому в даній роботі запропоновані зміни та доповнення на трьох циклах виконання цих робіт. Розроблені вимоги до комплексної системи захисту інформаційних ресурсів з врахуванням особливостей телекомунікаційної мережі, яка побудована за технологією IP/MPLS, та задач захисту державних інформаційних ресурсів. Наведені особливості реалізації КСЗІР в мережі.

В рамках окремого дослідження неможливо врахувати всі наявні методологічні рекомендації щодо захисту державних інформаційних ресурсів. Тому напрямом подальшої роботи може бути розробка науково-методичних основ та рекомендацій з побудови КСЗІР з врахуванням ієрархічних властивостей, розподіленого характеру та складності телекомунікаційної мережі.

Література: ***1.*** *Закон України «Про телекомунікації» // Відомості Верховної Ради (ВВР), в редакції Закону 2007, N 13, ст. 132.* ***2.*** *ДСТУ 3396.0-96. Технічний захист інформації. Основні положення. – С. 13.* ***3.*** *ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт. – С. 17.* ***4.*** *Кононович В. Г., Тардаскіна Т. М., Гладиш С. В. Реалізація концепції захисту інформаційних ресурсів у телекомунікаційній мережі загального користування // Зв'язок. – 2007. - №4. – с. 30 – 37.* ***5.*** *Олвейн В. Структура и релизация современной технологии MPLS / Пер. с англ. – М.: Изд. дом «Вильямс», 2004. – 480 с.* ***6.*** *Зайченко Е. Ю. Комплекс моделей и алгоритмов оптимизации характеристик сетей с технологией MPLS // Системні дослідження та інформаційні технології, 2007, № 4. – С. 58-71.* ***7.*** *Аленов О. М. Технология GMPLS: универсальная многопротокольная коммутация меток // Вестник связи № 8.–2002.– С. 28–37.* ***8.*** *Rosen E., Viswanathan A., R. Callon. Multiprotocol Label Switching Architecture. RFC 3031, January 2001.− С 61.* ***9.*** *Rosen E. RFC-3032. MPLS Label Stack Encoding. 2001. – С. 23.* ***10***. *Рекомендация МСЭ-Т G.8110/Y.1370. Архитектура сетей уровня MPLS. – 2005. – 72 с.* ***11.*** *Рекомендация МСЭ-Т Y.1561. Рабочие параметры и параметры доступности для сетей MPLS. – 2004. – 26 с.* ***12***. *Рекомендация МСЭ-Т Y.1711. Механизм эксплуатации и технического обслуживания для сетей MPLS. – 2004. – 36 с.* ***13***. *ITU-T Recommendation Y.1720. Protection switching for MPLS networks. – 2006. – 36 p.* ***14.*** *Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». В редакції Закону № 2594-IV від 31.05.2005. – С. 5.* ***15.*** *Рекомендация МСЭ-Т Е.408. Общая эксплуатация сети. Требования к безопасности сетей электросвязи. – 2004. – С. 21.* ***16.*** *ПРАВИЛА забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою КМУ № 373 від 29.04.06 – С. 4.* ***17.*** *НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом № 53 ДСТСЗІ СБУ від 4.12.2000. – С. 30.* ***18.*** *Рекомендация МСЭ-Т Е.409. Общая эксплуатация сети. Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи. – 2004. – С. 16.*

УДК:621.396.677.4; [539.37.38:621.396.946]

СПІРАЛЬНІ АНТЕНИ З РЕГУЛЬОВАНИМИ ХАРАКТЕРИСТИКАМИ

Юрій Міць
Запорізька державна інженерна академія

Анотація: **Розглядається можливість застосування просторової конічної періодичної спіральної антени з регульованими радіопеленгаційними характеристиками в сотовому телефоні спеціального призначення.**
Summary: **The usage of space conical periodical spiral antenna with regulation radio direction funding characteristics in cell radiotelephones of special assignment is considered.**
Ключові слова: **Сотовий телефон, спіральна антена, діаграма спрямованості.**

І Вступ

Ефективність технічного виявлення та термінового захисту несанкціонованого витоку конфіденційної інформації з сучасних електронних мереж, боротьба з хабарництвом, корупцією, організованою злочинністю та тероризмом тощо в сучасних умовах практично неможливі без використання спеціальних малогабаритних мобільних широкосмугових радіотехнічних систем навколоземного та космічного радіозв'язку, радіоастрономії, радіостеження, радіопеленгації, радіоборотьби, радіовимірювання, технічної радіорозвідки, заснованих на використанні малогабаритних надширокосмугових просторових спіральних антен з регульованими радіопеленгаційними характеристиками та параметрами зовнішнього поля випромінювання.

На тимчасову відсутність такої радіоапаратури можливо і продовжують розраховувати різні злочинні угрупування, плануючи проведення безвідповідальних терористичних актів. Відомо, наприклад, що один з таких терористичних актів відбувся у московському театральному центрі на Дубровці 23 – 26 жовтня 2004 р. ЗМІ повідомляли, що ФСБ Росії під час провадження терористами теракту мали лише можливість прослуховувати розмови замовників теракту та визначити приблизні координати розташування замовників теракту, але у ФСБ не було відповідних технічних засобів щодо вимірювання точних координат місця їх перебування (квартира, підвал, гараж тощо). Це позбавило ФСБ вийти на переговори з замовниками теракту щодо узгодження умов припинення терористами неконституційних дій та негайного визволення